UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

BERNADETTE BEEKMAN, ELIZABETH TWITCHELL JAMES FREEMAN-HARGIS, and DOUGLAS DIAMOND individually and on behalf of all others similarly situated, Plaintiffs, v. EQUIFAX INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Bernadette Beekman, Elizabeth Twitchell, James Freeman-Hargis, and Douglas Diamond ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, allege upon personal knowledge as to themselves, and upon information and belief as to all other matters, based upon the investigation made by and through their attorneys, as follows:

SUMMARY OF ACTION

1. On September 7, 2017, Equifax Inc. ("Equifax" or the "Company") disclosed a nationwide data breach affecting an estimated 143 million American consumers (the "Data Breach"). According to the press release published by

Equifax, criminals exploited a U.S. website application vulnerability to access the Company's consumer and commercial credit reporting databases from mid-May 2017 through July 2017. The information stolen primarily included names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, credit dispute documents, and other personally identifiable information (collectively, "PII").

2. Equifax purportedly discovered the unauthorized access to its databases as early as July 29, 2017 and engaged an independent cybersecurity firm to conduct a forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to its databases to law enforcement at this time. Unbelievably, however, Equifax chose not to inform consumers about this massive breach until September 7, 2017.

3. The Data Breach resulted from Equifax's failure to implement adequate security measures to safeguard consumers' PII and having willfully ignored *known* weaknesses in its data security, including prior hacks into its systems and those of its subsidiaries, along with the weaknesses those previous intrusions identified. Unauthorized parties routinely attempt to gain access to and steal information from networks and information systems – especially from entities

like Equifax, which are known to possess the valuable personal and financial information of a large number of individuals and entities.

4. As a result of Equifax's willful failure to prevent the breach, Plaintiffs and Class members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a heightened and imminent risk of such harm in the future.

5. Although Equifax claims that it has found no evidence of unauthorized activity on its core consumer or commercial credit reporting databases, Plaintiffs and other Class members will become victims of identity fraud in the future, given the breadth of the PII that was exposed during the Data Breach.

6. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance beyond Equifax's current one-year offer, and injunctive

relief including an order requiring Equifax to implement improved data security measures.

THE PARTIES

7. Plaintiff Bernadette Beekman ("Beekman") is a citizen of New York who resides in New York, New York. Although Ms. Beekman has occasionally obtained her credit report from Equifax, she has not subscribed to any of their credit monitoring services. On September 8, 2017, Ms. Beekman followed the instructions disseminated by Equifax to determine if her information had been potentially impacted and to sign up for credit file monitoring and identity theft protection. She was informed that her information had "most likely" been compromised and instructed to return to the website in a couple of days for more details on how to enroll in the free credit monitoring services to be offered by Equifax. When Ms. Beekman returned to the Equifax website later in the day, she was not yet able to continue with her enrollment.

8. Plaintiff Elizabeth Twitchell ("Twitchell") is a citizen of Virginia who resides in Alexandria, Virginia. Ms. Twitchell has never subscribed to any Equifax credit monitoring services. When she read the news of the Data Breach, however, she checked her status on the Equifax website and was informed that her information had likely been compromised.

9. Plaintiff James Freeman-Hargis ("Freeman-Hargis") is a citizen of Illinois who resides in Chicago, Illinois. Mr. Freeman-Hargis has never paid for credit monitoring services from Equifax, though he did receive free monitoring from the Company for one year in or around 2009, as a result of an unrelated data breach. Upon learning of the most recent Data Breach, Mr. Freeman-Hargis checked his status on the Equifax website and was informed that his information had likely been compromised.

10. Plaintiff Douglas Diamond ("Diamond") is a citizen of Oregon who resides in Portland, Oregon. Mr. Diamond has never purchased any credit monitoring services from Equifax. When he learned of the recent Data Breach, however, Mr. Diamond checked his status on the Equifax website and was informed that his PII had likely been compromised.

11. Defendant Equifax is a Georgia corporation with its principal place of business located at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. Equifax is one of the three major credit reporting bureaus in the United States. As a credit bureau service, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower. Its products and services are based on comprehensive databases of consumer and

business information derived from numerous sources including, credit, financial assets, telecommunications and utility payments, employment, income, demographic, and marketing data. The Company purports to assist consumers in understanding, managing, and protecting their personal information.

JURISDICTION AND VENUE

12. This Court has diversity jurisdiction over this class action pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and some members of the Classes (as defined below) are citizens of a different state than Defendant.

13. Additionally, pursuant to 28 U.S.C. § 1331, this Court has jurisdiction over Plaintiffs' claims under the FCRA, 15 U.S.C. §§ 1681e, *et seq*. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).

14. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b), because Equifax's principal place of business is in this District and a substantial part of the events or omissions that give rise to Plaintiffs' claims occurred in this District.

SUBSTANTIVE ALLEGATIONS

The Data Breach Compromised the PII of 143 Million American Consumers

15. On September 7, 2017, Equifax announced that its systems had been breached and that the Data Breach affected approximately 143 million consumers throughout the United States. According to the press release issued by the Company, unauthorized users exploited a vulnerability in Equifax's systems to gain access to PII including names, Social Security numbers, and addresses, among other sensitive personal information:

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially ***impacting approximately 143 million U.S. consumers***. Criminals exploited a U.S. ***website application vulnerability*** to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> ***The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.*** In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

Equifax ***discovered the unauthorized access on July 29*** of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3- Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447- 7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. - 1:00 a.m. Eastern time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of

> contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.
>
> Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.
>
> CEO Smith said, "I've told our entire team that our goal can't be simply to fix the problem and move on. Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, we recognize we must do more. And we will."[1]

16. Equifax is one of the three major credit reporting bureaus in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, including assisting organizations with evaluating the risks associated with providing credit to individuals and providing consumers with online access to their credit history and score. Equifax also maintains and is entrusted with PII related to the credit history of consumers, and provides this information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

[1] *See* Press Release, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, *available at* https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 (last visited Sept. 8, 2017).

17. Equifax gets its consumer PII from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies like Equifax, as well as by purchasing public records.

18. Moreover, although Equifax claims to be a leader in data security and in managing data breaches once they occur, and its privacy policy promises to reasonably safeguard consumer data, Equifax's own data security practices were woefully inadequate. Equifax was well aware of this fact because it had experienced multiple data breaches in recent years.

19. Equifax has a history of major data security blunders. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated, "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? They are first-hand delivering information for the fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau."[2]

20. In March 2013, Equifax confirmed "fraudulent and unauthorized" access to the credit reports of multiple celebrities and top Washington, D.C.

[2] *See* http://www.cnet.com/news/equifax-tax-forms-expose-worker-social-security-numbers/, last accessed May 9, 2016.

officials, including former First Lady Michelle Obama and former Vice President Joe Biden.[3]

21. In March 2015, Equifax notified certain consumers that personal information contained on their credit file was erroneously sent to unauthorized individuals due to a technical error during a software change.[4]

22. Also in March 2015, Equifax mistakenly sent a Maine woman the full credit reports of more than 300 other individuals, which exposed their SSNs, dates of birth, current and previous addresses, creditor information, and bank and loan account numbers, among other sensitive information. The woman told reporters, "I'm not supposed to have this information, this is unbelievable, someone has messed up."[5]

23. In 2016, Equifax suffered three data breaches relating to its W-2 database alone.

24. Cybersecurity professionals have been quick to criticize Equifax for not improving its security practices after those previous thefts.

---

[3] *See* http://www.reuters.com/article/us-usa-cybersecurity-hacking-idUSBRE92B12520130313, last accessed May 9, 2016.

[4] *See* http://doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf, last accessed May 9, 2016.

[5] *See* http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/, last accessed May 9, 2016.

25. In the press release announcing the Data Breach, Equifax's CEO claimed that the Company had "made significant investments in data security" and stated that Equifax "pride[s] [itself] on being a leader in managing and protecting data." Nevertheless, Equifax exposed consumers' most sensitive personal information to data breaches by failing to adequately implement the multiple layers of controls necessary to prevent this type of catastrophic damage.

The Data Breach Has Exposed Plaintiffs and Other Consumers to Heightened, Imminent Risk of Fraud, Identity Theft, and Financial Harm

26. Since identity thieves use the PII of other people to commit fraud or other crimes, Plaintiffs and other consumers whose information was exposed in the Data Breach are subject to an increased, imminent, and concrete risk of identity theft.

27. The exposure of Plaintiffs' and Class members' SSNs in particular poses serious problems. Criminals frequently use SSNs to create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name.

28. SSNs have become a default national identification number for most American citizens today. Consumer advocates have pointed out that "While the potential sources of SSNs are vast and accessible, you can take steps to keep your SSN out of the hands of potential thieves. Unfortunately, your SSN is often saved

in numerous databases which may be subject to compromise by hackers or other means. In recent years, news stories of data breaches in which SSNs are compromised are a daily occurrence."[6]

29. In fact, SSNs can even be guessed "with startling accuracy" based on a person's birthdate and state of birth.[7]

30. Security experts have pointed out that Social Security numbers "were never intended to be secure", and in fact, have been assigned largely based on a geographical and sequential system.[8]

31. As a result of the theft of their PII, Plaintiffs and the other Class members have suffered one or a combination of the following injuries:

(a) incidences of identity fraud and theft, including unauthorized bank activity, fraudulent credit card purchases, and damage to their credit;

(b) money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of PII;

---

[6] *See* https://www.privacyrights.org/my-social-security-number-how-secure-it, last accessed May 9, 2016.

[7] *See* http://www.slate.com/articles/technology/webhead/2009/07/no_you_cant_have_my_social_security_number.html, last accessed May 9, 2016

[8] *Id.*

(c) lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach including, but not limited to, efforts to research how to prevent, detect, contest, and recover from misuse of their PII; and

(d) loss of the opportunity to control how their PII is used.

32. Furthermore, Plaintiffs and Class members have suffered, and/or will face an increased risk of suffering in the future, the following injuries:

(a) money and time lost as a result of fraudulent access to and use of their financial accounts;

(b) loss of use of and access to their financial accounts and/or credit;

(c) impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

(d) lowered credit scores resulting from credit inquiries following fraudulent activities;

(e) costs and lost time obtaining credit reports in order to monitor their credit records;

(f) money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

(g) money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

(h) costs of credit monitoring that is more robust than the limited services being offered by Equifax;

(i) anticipated future costs from the purchase of credit monitoring and/or identity theft protection services once the temporary services being offered by Equifax expire;

(j) costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

(k) money and time expended to ameliorate the consequences of the filing of fraudulent tax returns; and

(l) continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

33. The risks that Plaintiffs and Class members bear as a result of the Data Breach cannot be mitigated by the limited credit monitoring Equifax has offered to affected consumers because it can only help detect, but will not prevent, the fraudulent use of Plaintiffs' and Class members' PII. Instead, Plaintiffs and Class members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiffs and Class members.

Equifax Failed to Ensure the Security of Plaintiffs' PII and to Investigate and Provide Timely and Adequate Notification of the Data Breach as Required by Federal Regulations

34. In addition to the requirements of the FCRA, and several state statutes (discussed below), the Gramm-Leach-Bliley Act ("GLBA") imposes upon financial institutions (of which Equifax qualifies under the statute) "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b).

35. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

36. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* At a ***minimum***, an institution's response program should contain procedures for, *inter alia*, identifying the nature and scope of an incident, notifying its primary federal regulator as soon as possible, taking

appropriate steps to control the incident to prevent further unauthorized access, and notifying customers of the breach.

37. Credit bureaus like Equifax are "financial institutions" for purposes of the GLBA and are, therefore, subject to its provisions. "Nonpublic personal information," incudes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for the purposes of the Interagency Guidelines Establishing Information Security Standards.

38. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to: (a) implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiffs' and Class members' PII.

39. Equifax also failed to notify affected consumers as soon as possible after it became aware of unauthorized access to sensitive customer information.

Equifax became aware of the Data Breach no later than July 29, 2017, but did not inform consumers of the breach until September 7, 2017.

40. Further demonstrating the callousness of Equifax's management and that the Company's executives were more interested in lining their own pockets than in safeguarding customers' sensitive personal information, on August 1 and 2, 2017, mere days after Equifax's discovery of the Data Breach, three Equifax executives offloaded shares cumulatively worth approximately $1.8 million.[9] These shares were reportedly sold on the open market, not pursuant to any scheduled sales plan. Accordingly, though having placed millions of Americans and their families at financial risk, Equifax's executives cashed out before announcing the Data Breach to the hundreds of millions of Americans whose personal information was stolen.

CLASS ACTION ALLEGATIONS

41. Plaintiffs bring all claims set forth below as class claims, pursuant to Federal Rules of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4) on behalf of the following classes (hereinafter, the "Class" or the "Classes"):

[9] According to recent reports, Chief Financial Officer John Gamble reportedly sold approximately $946,374 of Equifax stock, Workforce Solutions President Rodolfo Ploder sold shares worth about $254,458, and U.S. Information Solutions President Joseph Loughran cashed in approximately $584,099 worth of Equifax stock.

Nationwide Class

All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

Illinois Subclass

All persons residing in Illinois whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

New York Subclass

All persons residing in New York whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

Oregon Subclass

All persons residing in Oregon whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

Virginia Subclass

All persons residing in Virginia whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax on September 7, 2017.

42. Excluded from the Classes are employees or agents of Equifax and its subsidiaries and affiliates, all persons who make a timely request to be excluded from the Classes, and the Court and its employees, officers, and relatives.

43. Plaintiffs hereby reserve the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery.

44. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis, using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

45. This action has been brought and may be properly maintained on behalf of the Classes proposed herein under Federal Rule of Civil Procedure 23.

46. **Numerosity.** The members of the Classes are so numerous and geographically dispersed that individual joinder of all members of the Classes is impracticable. According to Equifax, the Nationwide Class includes approximately 143 million individuals throughout the United States whose PII was acquired during the Data Breach. On information and belief, Plaintiffs allege that there are also thousands to millions of individuals in each State Subclass. The parties will be able to identify each member of the Classes after Defendants' document production and/or related discovery.

47. **Commonality.** This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

(a) Whether Equifax engaged in the wrongful conduct alleged herein;

(b) Whether Equifax owed a duty to Plaintiffs and Class members to adequately protect their PII;

(c) Whether Equifax breached its duties to protect the sensitive personal information of Plaintiffs and Class members;

(d) Whether Equifax knew or should have known that its data security systems and processes were vulnerable to attack;

(e) Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Equifax's conduct including, *inter alia*, increased risk of identity theft;

(f) Whether Equifax violated the FCRA; and

(g) Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief.

48. **Typicality.** Plaintiffs' claims are typical of the claims of other Class members because, among other things, all Class members were comparably injured through the wrongful conduct of Equifax, as described above. Each of the

Plaintiffs, like all proposed Class members, had his or her PII compromised in the Data Breach.

49. **Adequacy.** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other members of the Classes they seek to represent. Furthermore, Plaintiffs have retained counsel competent and experienced in complex class action litigation. The Classes' interests will be fairly and adequately protected by Plaintiffs, who intend to prosecute this action vigorously, and by Plaintiffs' skilled and experienced counsel.

50. **Predominance.** The proposed class action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Classes predominate over any questions that may affect only individual Class members.

51. **Superiority.** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Classes are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it

would be impracticable for members of the Classes to individually seek redress for Equifax's wrongful conduct.

52. Even if Class members could afford individual litigation, the court system could not. Individual litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and to the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

53. **Injunctive & Declaratory Relief.** Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Classes, thereby making appropriate final injunctive and declaratory relief, as described below, with respect to the Classes as a whole.

54. **Certification of Particular Issues.** Particular issues are appropriate for certification under Federal Rule of Civil Procedure 23(c)(4) because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

(a) Whether Equifax failed to timely notify Plaintiffs and the Class of the Data Breach;

(b) Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

(c) Whether Equifax's security measures were reasonable in light of data security recommendations and other measures recommended by data security experts;

(d) Whether Equifax failed to adequately comply with industry standards amounting to negligence;

(e) Whether Equifax failed to take commercially reasonable steps to safeguard the PII of Plaintiffs and the other Class members; and

(f) Whether adherence to data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

55. **Discovery Rule Tolling:** Even through the exercise of reasonable diligence, Plaintiffs and other members of the Classes could not have reasonably discovered, and could not have known of facts that would have caused a reasonable person to suspect (within any applicable statute of limitations), that their PII had been collected by unauthorized users for several months. Even a reasonable and diligent investigation by Plaintiffs or other members of the Classes could not have revealed that Equifax had information in its possession about the

Data Breach, which was discovered by Plaintiffs only very shortly before this action was filed.

CLAIMS FOR RELIEF

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On Behalf of the Nationwide Class)

56. Plaintiffs incorporate by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

57. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

58. Under the FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

59. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

60. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

61. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

62. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

63. As a consumer reporting agency, Equifax may only furnish a

consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

64. Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

65. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take

adequate measures to fulfill their obligations to protect information contained in consumer reports, as required" by the FCRA, in connection with data breaches.[10]

66. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, Equifax's other data breaches in the past. Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

67. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of

[10] Statement of Commissioner Brill (Federal Trade Commission 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf (last visited Sept. 8, 2017).

their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the Classes of their rights under the FCRA.

68. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under the FCRA.

69. Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

70. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

COUNT II
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On Behalf of the Nationwide Class)

71. Plaintiffs incorporate by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

72. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, Equifax's other data breaches in the past. Further, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

73. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

74. Plaintiffs and the Nationwide Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

75. Plaintiffs and the Nationwide Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III
NEGLIGENCE
(On Behalf of the Nationwide Class & Each State Subclass)

76. Plaintiffs incorporate by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

77. Equifax owed a duty to Plaintiffs and Class members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class members' information was adequately secured from unauthorized access.

78. Equifax owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

79. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

80. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class members' PII.

81. Equifax also had independent duties under Plaintiffs' and Class members' state laws that required the Company to reasonably safeguard Plaintiffs' and Class members' PII and promptly notify them about the Data Breach.

82. Equifax's role to utilize and purportedly safeguard Plaintiffs' and Class members' PII presents unique circumstances requiring a reallocation of risk.

83. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that the Company's data security practices were inadequate to safeguard Class members' PII; and (d) failing to provide adequate and timely notice of the Data Breach.

84. But for Equifax's breach of its duties, Class members' PII would not have been accessed by unauthorized individuals.

85. Plaintiffs and Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

86. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII for no permissible purposes under the FCRA.

87. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class members' PII has also diminished the value of the PII.

88. The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

89. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT IV
NEGLIGENCE PER SE
(On Behalf of the Nationwide Class & Each State Subclass)

90. Plaintiffs incorporate by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

91. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

92. Equifax failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

93. Plaintiffs and Class members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

94. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (4) to insure the security and confidentiality of customer records and information;

> (5) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (6) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b) (emphasis added).

95. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

96. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

97. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or

will be misused" ***and*** "notif[ied] the affected customer[s] as soon as possible." *See id*.

98. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' PII, failure to detect the Data Breach in a timely manner, and failure to disclose that Defendants' data security practices were inadequate to safeguard Class members' PII.

99. Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

100. Plaintiffs and Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify Class members of the Data Breach would cause damages to Class members.

101. Equifax's failure to comply with the applicable laws and regulations, including the FCRA and the GLBA, constitutes negligence per se.

102. But for Equifax's violation of the applicable laws and regulations, Class members' PII would not have been accessed by unauthorized individuals.

103. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class members' PII has also diminished the value of the PII.

104. The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

105. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT V
VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT
815 Ill. Comp. Stat. § 505/1, *et seq*.
(On Behalf of the Illinois Subclass)

106. Plaintiff James Freeman-Hargis incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

107. Equifax, while operating in Illinois, employed unfair and deceptive acts and practices, including deception and misrepresentation, in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. 505/2. This includes but is not limited to the following:

a) Equifax failed to enact adequate privacy and security measures to protect the Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b) Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to

safeguard Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d) Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Illinois Subclass members' PII;

e) Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass members' PII, including but not limited to duties imposed by the FCRA, the GLBA, Illinois laws regulating the use and disclosure of Social Security numbers (815 Ill. Comp. Stat. 505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. 510/2(a));

f) Equifax failed to maintain the privacy and security of Illinois Subclass members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

g) Equifax failed to disclose the Data Breach to Illinois Subclass members in a timely and accurate manner, including in violation of the duties

imposed by 815 Ill. Comp. Stat. § 530/10(a).

108. As a direct and proximate result of Equifax's practices, the Illinois Subclass members suffered injuries to legally protected interests, as described above, including their legally protected interest in the confidentiality and privacy of their PII, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

109. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that the Illinois Subclass members could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

110. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Illinois Subclass members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Subclass.

111. Plaintiff James Freeman-Hargis and the Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 505/10a, including but not limited to

damages, restitution and punitive damages (to be proven at trial), injunctive relief, and/or attorneys' fees and costs.

COUNT VI
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. § 505/2, *et seq*.
(On Behalf of the Illinois Subclass)

112. Plaintiff James Freeman-Hargis incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

113. Equifax, while operating in Illinois, engaged in deceptive trade practices in the course of its business and vocation, in violation of 815 Ill. Comp. Stat. § 510/2(a), including representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised. This includes but is not limited to the following:

a) Equifax failed to enact adequate privacy and security measures to protect the Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b) Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d) Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Illinois Subclass members' PII;

e) Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the GLBA, 15 U.S.C. § 6801 *et seq*., Illinois laws regulating the use and disclosure of Social Security numbers, 815 Ill. Comp. Stat. 505/2RR, and the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/1 *et seq*.;

f) Equifax failed to maintain the privacy and security of Illinois Subclass members' PII, in violation of duties imposed by applicable federal and

state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

g) Equifax failed to disclose the Data Breach to Illinois Subclass members in a timely and accurate manner, including in violation of the duties imposed by 815 Ill. Comp. Stat. § 530/10(a).

114. Equifax knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

115. Illinois Subclass members were likely to be damaged by Equifax's deceptive trade practices, which Equifax knew or should have known.

116. Plaintiff James Freeman-Hargis and the Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 510, including, but not limited to, injunctive relief and attorney's fees.

COUNT VII
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law § 349
(On Behalf of the New York Subclass)

117. Plaintiff Bernadette Beekman incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

118. Equifax, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a) Equifax failed to enact adequate privacy and security measures to protect the New York Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b) Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the New York Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d) Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the New York Subclass members' PII;

e) Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the New York Subclass members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

f) Equifax failed to maintain the privacy and security of the New York Subclass members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

g) Equifax failed to disclose the Data Breach to the New York Subclass members in a timely and accurate manner, including in violation of the duties imposed by N.Y. Gen Bus. Law § 899-aa(2).

119. As a direct and proximate result of Equifax's practices, the New York Subclass members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

120. The above unfair and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the New York Subclass members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

121. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the New York Subclass members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

122. Plaintiff Bernadette Beekman and the New York Subclass members seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT VIII
VIOLATION OF THE OREGON UNLAWFUL TRADE PRACTICES ACT
Or. Rev. Stat. § 646.608, *et seq*.
(On Behalf of the Oregon Subclass)

123. Plaintiff Douglas Diamond incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

124. While operating in Oregon, Equifax engaged in deceptive trade practices in the course of its business and occupation, including by representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, advertising its services with intent not to sell them as advertised, and engaging in other unfair and deceptive conduct in trade or commerce, in violation of Or. Rev. Stat. § 646.608(1)(e), (g), and (u). This includes, but is not limited to, the following:

(a) Equifax failed to enact adequate privacy and security measures to protect the Oregon Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

(b) Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

(c) Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Oregon Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

(d) Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Oregon Subclass members' PII;

(e) Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Oregon Subclass members' PII including, but not limited to, duties imposed by the FCRA and the GLBA;

(f) Equifax failed to maintain the privacy and security of the Oregon Subclass members' PII, in violation of duties imposed by applicable federal and state laws including, but not limited to, those mentioned in the foregoing paragraph, directly and proximately causing the Data Breach;

(g) Equifax violated the Oregon Consumer Identity Theft Protection Act, Or. Rev. Stat Ann. §§ 646A.600, *et seq*., as alleged in more detail below; and

(h) Equifax failed to disclose the Data Breach to the Oregon Subclass members in a timely and accurate manner, including in violation of the duties imposed by Or. Rev. Stat. Ann. § 646A.604(1).

125. As a direct and proximate result of Equifax's practices, the Oregon Subclass members suffered injury and/or damages including, but not limited to,

time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

126. The above unfair and deceptive acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Oregon Subclass members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

127. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Oregon Subclass members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful.

128. Plaintiff Douglas Diamond and the Oregon Subclass seek all remedies available under Or. Rev. Stat. § 646.638, including equitable relief, actual damages, statutory damages of $200 per violation, and/or punitive damages.

129. Plaintiff Douglas Diamond and the Oregon Subclass also seek reasonable attorneys' fees and costs under Or. Rev. Stat. § 646.638(3).

COUNT IX
VIOLATION OF THE OREGON CONSUMER IDENTITY THEFT PROTECTION ACT
Or. Rev. Stat. § 646A.600, *et seq*.
(On Behalf of the Oregon Subclass)

130. Plaintiff Douglas Diamond incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

131. Pursuant to Or. Rev. Stat. Ann. § 646A.622(1), a business "that maintains records which contain personal information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

132. Equifax is a business that maintains records which contain personal information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiff Douglas Diamond and the other Oregon Subclass members.

133. Equifax violated Or. Rev. Stat. Ann. § 646A.622(1) by failing to implement reasonable measures to protect Oregon Subclass members' PII.

134. Equifax was required to accurately notify Oregon Subclass members when Equifax became aware of the Data Breach, in the most expeditious time

possible and without unreasonable delay pursuant to Or. Rev. Stat. Ann. § 646A.604(1).

135. Equifax is a business that owns, maintains, or otherwise possesses data that includes consumers' personal information as defined by Or. Rev. Stat. Ann. § 646A.604(1).

136. Oregon Subclass members' PII (*e.g.*, SSNs) includes personal information as covered by Or. Rev. Stat. Ann. § 646A.604(1).

137. Because Equifax discovered a breach of its security system, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Or. Rev. Stat. Ann. § 646A.604(1).

138. As a direct and proximate result of Equifax's violations of Or. Rev. Stat. Ann. §§ 646A.604(1) and 646A.622(1), Plaintiff Douglas Diamond and Oregon Subclass members suffered damages, as described above.

139. Equifax's failure to implement reasonable security measures, to promptly notify Plaintiff Douglas Diamond and other Oregon Subclass members, and otherwise to comply with Or. Rev. Stat. Ann. § 646A.600, *et seq*., constitutes unlawful, unfair, and deceptive practices including under Or. Rev. Stat. Ann. § 646.607(9).

140. Plaintiff Douglas Diamond and the other Oregon Subclass members seek compensation for affected consumers pursuant to Or. Rev. Stat. Ann. § 646A.624(3), because enforcement of the rights of the consumers though this private civil action is feasible, and not so burdensome or expensive as to be impractical.

141. Plaintiff Douglas Diamond and the members of the Oregon Subclass seek relief under Or. Rev. Stat. Ann. § 646A.624(3) including, but not limited to, actual damages and injunctive relief.

COUNT X
VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT
Va. Code Ann. § 59.1-196, *et seq*.
(On Behalf of the Virginia Subclass)

142. Plaintiff Elizabeth Twitchell incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

143. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

144. Equifax compiled, maintained, used, and furnished Plaintiffs' and Virginia Subclass members' PII in connection with consumer transactions, as defined under Va. Code Ann. § 59.1-198.

145. While operating in Virginia, Equifax engaged in deceptive trade practices in connection with consumer transactions, including by representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised, in violation of Va. Code Ann. § 59.1-200. This includes but is not limited to the following:

a) Equifax failed to enact adequate privacy and security measures to protect the Virginia Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b) Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Virginia Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d) Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Virginia Subclass members' PII;

e) Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Virginia Subclass members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq*.;

f) Equifax failed to maintain the privacy and security of Virginia Subclass members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

g) Equifax filed to disclose the Data Breach to the Virginia Subclass members in a timely and accurate manner, including in violation of the duties imposed by Va. Code Ann. § 18.2-186.6.

146. As a direct and proximate result of Equifax's practices, Plaintiff Elizabeth Twitchell and Virginia Subclass members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their

financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

147. The above unfair and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Virginia Subclass members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

148. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Virginia Subclass members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

149. Plaintiff Elizabeth Twitchell and Virginia Subclass members seek all available relief under Va. Code Ann. § 59.1-204, including, but not limited to, actual damages; statutory damages and/or penalties in the amount of $1,000 per violation or, in the alternative, $500 per violation; restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

COUNT XI
VIOLATION OF THE VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT
Va. Code Ann. § 18.2-186.6, *et seq*.
(On Behalf of the Virginia Subclass)

150. Plaintiff Elizabeth Twitchell incorporates by reference the allegations made in paragraphs 1 through 55 as if fully set forth herein.

151. Equifax is required to accurately notify Plaintiffs and Virginia Subclass members following discovery or notification of a breach of its data security system (if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud) without unreasonable delay pursuant to Va. Code Ann. § 18.2-186.6(B).

152. Equifax is an entity that owns, licenses, or maintains computerized data that includes personal information as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

153. Plaintiff and Virginia Subclass members' PII (*e.g.*, Social Security numbers) includes personal information as covered under Va. Code Ann. § 18.2-186.6(A).

154. Because Equifax discovered a breach of its security system (in which unencrypted or unredacted personal information was or is reasonably believed to

have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B) and/or 18.2-186.6(D).

155. As a direct and proximate result of Equifax's violations of Va. Code Ann. §§ 18.2-186.6(B) and/or 18.2-186.6(D), Plaintiffs and Virginia Subclass members suffered damages, as described above.

156. Plaintiff Elizabeth Twitchell and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including, but not limited to, damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court, on behalf of themselves and all others similarly situated, enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class and State Subclasses as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and State Subclasses requested herein;

B. Injunctive relief requiring Equifax to: (1) strengthen its data security systems that maintain PII to comply with the FCRA and GLBA, the applicable state laws alleged herein, and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on the Company's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; (4) provide direct, written notice of the Data Breach to all affected persons, which includes a full description of the breadth, scope, and risks of the data breach; and (5) routinely and continually conduct training to inform internal security personnel how to prevent, identify, and contain a breach, and how to appropriately respond thereto;

C. An order requiring Equifax to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiffs and all Class members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiffs and all Class members of additional credit monitoring and identity theft protection services beyond the one-year package Equifax is currently offering;

F. An award of the costs and expenses of this litigation, including reasonable attorneys' fees, experts' fees, and other costs and disbursements;

G. An order requiring Equifax to pay pre- and post-judgment interest, as provided by law or equity; and

H. An award of such other and further relief as may be just and proper under the circumstances.

JURY DEMAND

Plaintiffs hereby demand a trial by jury.

Respectfully submitted this 12th day of September, 2017.

LAW OFFICES OF DAVID A. BAIN, LLC

By: /s/ *David A. Bain*
David A. Bain
Georgia Bar No. 032449
1230 Peachtree Street
Suite 1050
Atlanta, GA 30309
Tel.: (404) 724-9990
Fax: (404) 724-9986
dbain@bain-law.com

BLOOD HURST & O'REARDON LLP
Timothy G. Blood
Thomas J. O'Reardon II
701 B Street, Suite 1700
San Diego, CA 92101
Tel.: (619) 338-1100
Fax: (619) 338-1101
tblood@bholaw.com
toreardon@bholaw.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
Janine L. Pollack
Thomas H. Burt
Correy A. Kamin
270 Madison Avenue
New York, NY 10016
Tel.: (212) 545-4600
Fax: (212) 686-0114
pollack@whafh.com
burt@whafh.com
kamin@whafh.com

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
Carl V. Malmstrom
70 West Madison Street, Suite 1400
Chicago, IL 60602
Tel.: (312) 984-0000
Fax: (312) 214-3110
malmstrom@whafh.com

Attorneys for Plaintiffs